Computer Security

Course Project (TEST Report)

Dr. Samer Khasawneh

Student name	Student ID
Moath AL-tahrawi	2141099
Sultan AL- Awawdah	1932354

1) Data confidentiality assurance by symmetric encryption.

ENCRYPTION PROCESS (ECB AND CBC):

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 1

Select action:
1. Encrypt
2. Decrypt
Enter your choice: 1
Enter plaintext: Hi, I am a computer engineer, i am studying computer security
Enter 8-byte key: qwerasdf

Encrypting using ECB mode...
ECB Ciphertext: da9fc299ec221c84fc17af2395a15fee70378875a63d12649af3ab6d2c8f55385302c0acf4a8c215f694e38aef841b6668fd1926c
9a315b8e37571c4f19d919f

Select another DES mode (CBC, CFB, OFB):
Enter mode: CBC
Generated IV/Nonce: 3aec3d79ee84d11e

Encrypting using CBC mode...
CBC Ciphertext: 517d3f58f18cce4cafe8bd8a67a43ced1db510e1adc26f1384b95ac4a1698acbee43a420d8a5436a49317ec2b2f3daa08fb7cd737
97e63eec96123ac0ac900ed
```

DECRYPTION PROCESS (ECB):

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 1

Select action:
1. Encrypt
2. Decrypt
Enter your choice: 2
Enter ciphertext (hex): da9fc299ec221c84fc17af2395a15fee70378875a63d12649af3ab6d2c8f55385302c0acf4a8c215f694e38aef841b666
8fd1926c9a315b8e37571c4f19d919f
Enter 8-byte key: qwerasdf

Select DES mode (ECB, CBC, CFB, OFB):
Enter mode: ECB
Decrypting using ECB mode...
Decrypted Text: Hi, I am a computer engineer, i am studying computer security
```

DECRYPTION PROCESS (CBC):

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 1

Select action:
1. Encrypt
2. Decrypt
Enter your choice: 2
Enter ciphertext (hex): 517d3f58f18cce4cafe8bd8a67a43ced1db510e1adc26f1384b95ac4a1698acbee43a420d8a5436a49317ec2b2f3daa08
fb7cd73797e63eec96123ac0ac900ed
Enter 8-byte key: qwerasdf

Select DES mode (ECB, CBC, CFB, OFB):
Enter mode: CBC
Enter IV/Nonce (hex): 3aec3d79ee84d11e
Decrypting using CBC mode...
Decrypted Text: Hi, I am a computer engineer, i am studying computer security
```

ENCRYPTION PROCESS (ECB AND OFB):

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 1

Select action:
1. Encrypt
2. Decrypt
Enter your choice: 1
Enter plaintext: Hi, I am a computer engineer, i am studying computer security
Enter 8-byte key: qwerasdf

Encrypting using ECB mode...
ECB Ciphertext: da9fc299ec221c84fc17af2395a15fee70378875a63d12649af3ab6d2c8f55385302c0acf4a8c215f694e38aef841b6668fd1926c
9a315b8e37571c4f19d919f

Select another DES mode (CBC, CFB, OFB):
Enter mode: OFB
Generated IV/Nonce: 98788efd236339aa

Encrypting using OFB mode...
OFB Ciphertext: 9858b37035df870ded499319c2b28f14405b0f454bee9de5a0a696e1aedaeae836781917f2c34eed23fd71ace213235176a1e58ec
c1c763f047e78565a927fb8
```

DECRYPTION PROCESS (OFB):

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 1

Select action:
1. Encrypt
2. Decrypt
Enter your choice: 2
Enter ciphertext (hex): 9858b37035df870ded499319c2b28f14405b0f454bee9de5a0a696e1aedaeae836781917f2c34eed23fd71ace21323517
6a1e58ecc1c763f047e78565a927fb8
Enter 8-byte key: qwerasdf

Select DES mode (ECB, CBC, CFB, OFB):
Enter mode: OFB
Enter IV/Nonce (hex): 98788efd236339aa
Decrypting using OFB mode...
Decrypted Text: Hi, I am a computer engineer, i am studying computer security
```

ENCRYPTION PROCESS (ECB AND CFB):

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 1

Select action:
1. Encrypt
2. Decrypt
Enter your choice: 1
Enter plaintext: Hi, I am a computer engineer, i am studying computer security
Enter 8-byte key: qwerasdf

Encrypting using ECB mode...
ECB Ciphertext: da9fc299ec221c84fc17af2395a15fee70378875a63d12649af3ab6d2c8f55385302c0acf4a8c215f694e38aef841b6668fd1926c
9a315b8e37571c4f19d919f

Select another DES mode (CBC, CFB, OFB):
Enter mode: CFB
Generated IV/Nonce: 5670249e14cf2a16

Encrypting using CFB mode...
CFB Ciphertext: 6924636369eb9906c0cfe249298b2dd186f23ddbe1510524431ad9db6443a3f273e701d2c726c6b0c6461e123712792f2188a4f58
f4fd426eae30aa306841470
```

DECRYPTION PROCESS (CFB):

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 1

Select action:
1. Encrypt
2. Decrypt
Enter your choice: 2
Enter ciphertext (hex): 6924636369eb9906c0cfe249298b2dd186f23ddbe1510524431ad9db6443a3f273e701d2c726c6b0c6461e123712792f2
188a4f58f4fd426eae30aa306841470
Enter 8-byte key: qwerasdf

Select DES mode (ECB, CBC, CFB, OFB):
Enter mode: CFB
Enter IV/Nonce (hex): 5670249e14cf2a16
Decrypting using CFB mode...
Decrypted Text: Hi, I am a computer engineer, i am studying computer security
```

2) Data confidentiality assurance by hybrid encryption (digital envelop)

ASSYMMETRIC KEY GENERATAION

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 2
1. Generate Key Pair
2. Encrypt
3. Decrypt
Enter your choice (1/2/3): 1
Key pair generated and saved to 'private_key.pem' and 'public_key.pem'.
```

ENCRYPTION (CREATING DIGITAL ENVELOPE)

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 2
1. Generate Key Pair
2. Encrypt
3. Decrypt
Enter your choice (1/2/3): 2
Enter plaintext to encrypt: Hi,I am a computer engineer, I study computer security
Enter the path to the receiver's public key file: public_key.pem
Encrypted Data:
Encrypted Key: vm2OvXyspfpUeaDlKIkfz4zOdgpSb1iaaorBNjAnHiO7fRTSywoijep5g+c7it47NIfV/yjiLrDQw6EgCphS9KShWyL2Sd4CpSW5NDh4r60SbdpEilO3p3He+K/
oSwYzIbmJB23TeGsJqLZW0RVO4CL4EbxpwaUkakG4InvX9qEx60IzCjghvf+YQOXU+sghbKT3UKSnwfh4TfuIthlHfUADiNocatZTEce1O98+vUO06ymDmy3Va60fJEqCSdTE0Y54p
V/qdxXa/D9sIO6o9oQfDJtgg2SL6H+/nVT2XBFsjVxxznJh79XJbbjvO9YFKjpfN27+R8rVH/MkhBmbKQ==
Nonce: S6K5cbY7eVA4U7lflmwYCw==
Ciphertext: tznH+VUckh2zBG8jnRGthRMkChAtbN9yYLXr8WGmTaibiHCXWqBwIbpwomMivQiEs6E+ytgypA==
```

DECRYPTION

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 2
1. Generate Key Pair
2. Encrypt
3. Decrypt
Enter your choice (1/2/3): 3
Enter the encrypted key: vm2OvXyspfpUeaDlKIkfz4zOdgpSb1iaaorBNjAnHiO7fRTSywoijep5g+c7it47NIfV/yjiLrDQw6EgCphS9KShWyL2Sd4CpSW5NDh4r60SbdpEi
lO3p3He+K/oSwYzIbmJB23TeGsJqLZW0RVO4CL4EbxpwaUkakG4InvX9qEx60IzCjghvf+YQOXU+sghbKT3UKSnwfh4TfuIthlHfUADiNocatZTEce1O98+vUO06ymDmy3Va60fJEq
CSdTE0Y54pV/qdxXa/D9sIO6o9oQfDJtgg2SL6H+/nVT2XBFsjVxxznJh79XJbbjvO9YFKjpfN27+R8rVH/MkhBmbKQ==
Enter the nonce: S6K5cbY7eVA4U7lflmwYCw==
Enter the ciphertext: tznH+VUckh2zBG8jnRGthRMkChAtbN9yYLXr8WGmTaibiHCXWqBwIbpwomMivQiEs6E+ytgypA==
Enter the path to the receiver's private key file: private_key.pem
Decrypted Text: Hi,I am a computer engineer, I study computer security
```

3) Message Authentication assurance.

MAC GENERATION

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 3
1. Generate MAC
2. Verify MAC
Enter your choice (1/2): 1
Enter a message: Hi, I am a Computer Engineer, I study Computer security
Authenticated Message with MAC: Hi, I am a Computer Engineer, I study Computer security |1734823596|23ba10c5a7afeeb0dff809c0bc548d02cc93ae
c6238241d0960e71caf554eb26
```

MAC VERIFICATION (REPLAY ATTACK DETECTED)

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 3
1. Generate MAC
2. Verify MAC
Enter your choice (1/2): 2
Enter the message with MAC: Hi, I am a Computer Engineer, I study Computer security |1734823596|23ba10c5a7afeeb0dff809c0bc548d02cc93aec623
8241d0960e71caf554eb26
MAC valid, but replay attack detected.
```

VERIFICATION OF A VALID MAC

```
Cryptographic Toolkit, choose one of the solutions below:
1. Data confidentiality assurance by symmetric encryption
2. Data confidentiality assurance by hybrid encryption (digital envelope).
3. Message Authentication assurance.
Enter your choice: 3
1. Generate MAC
2. Verify MAC
Enter your choice (1/2): 2
Enter the message with MAC: MOATH|1734823821|5e732632d73f0b28d3936bfc53a764404513d236d5b3432f7da5aa57b10e2cf9
MAC valid and message authenticated.
```